REMARKS

In this Amendment, Applicant has amended Claim 3 to correct a clerical error. It is respectfully submitted that no new matter has been introduced by the amended claim. All claims are now present for examination and favorable reconsideration is respectfully requested in view of the preceding amendments and the following comments.

CLAIM OBJECTIONS:

Claim 2 has been objected as containing informalities.

It is respectfully submits that the informalities indicated by the Examiner are in Claim 3. Claim 3 has been amended to correct the spelling for "subkey."

Therefore, withdrawal of the objection is respectfully requested.

REJECTIONS UNDER 35 U.S.C. § 102:

Claims 1 – 3 have been rejected under 35 U.S.C. § 102 (b) as allegedly being anticipated by Schneier (Bruce Schneier, Applied Cryptography, 1996, John Wiley & Sons).

Applicant traverses the rejection and respectfully submits that the present-claimed invention is not anticipated by the cited reference. More specifically, the embodiment of the present invention as defined in Claims 1 – 3 include the feature of "prior to carrying out said two-place operation on i-th subblock and subkey, a substitution operation is performed on the subkey **depending on** j-th subblock, where i ≠ j." (emphasis added) Such feature is not disclosed or taught by Schneier.

After studied the Schneier in detail, the Applicant respectfully submits that Fig.12.1 of Schneier shows a general diagram of data conversion in accordance with the

encryption algorithm DES (US Data Encryption Standard), which includes 16 rounds of conversion. In each round of conversion, based on a right subblock R and subkey K, function $f = f(R, K)$ is calculated, after which a left subblock L is converted by performing on it the operation XOR: $L: = L \oplus f(R, K)$, where ": =" is the designation of assignment operation. Between the preceding and subsequent encryption rounds, the subblocks are permutated. Thus, it is important to ascertain, how conversion $f(R, K)$ is performed. In the Examiner's view, in calculating $f(R, K)$, the operation of permuting subkey bits **depending on data subblock** is used. However, Applicant's detailed study of Schneier has shown that this is not the case. More specifically, Schneier shows that the procedures of calculating the function $f(R, K)$ includes consecutive performing the following operations:

- operation of broadening L 32-bit data subblock to X broadened 48-bit data subblock;

- conversion of the broadened subblock by means of its addition with 48-bit subkey $X : = X \oplus K$ (before this step, no conversions depending on the data block being converted have been performed on this round subkey, i.e. **no transmuting subkey bits depending on data has been performed**);

- performing a cascade of substitution operations of 6x4 size implementing the substitution operation S_{6x4}, as a result of which the broadened 48-bit subblock is converted into 32-bit binary vector $Z : Z = S_{6x4}(X)$;

- performing the transmutation operation P which consists in a fixed transmutation vector Z bits, i.e. transmutation vector Z bits independently of the value of some data subblock but always in the same manner, as prescribed by Table 12.7 at page 277 of the Schneier reference. After performing operation P, the value of $f(R, K)$ is obtained, i.e. we have $f(R, K) = P(Z)$.

The above detailed operations have revealed that, in forming the value of $f(R, K)$ in the DES algorithm, **the operation of transmuting subkey bits depending on data being converted is not used**. The vector Z bit transmuting operation performed in the cited method of block encryption (algorithm DES) is fixed and is performed **regardless**

of data being converted. Schneier confirms this by describing the operation P in the section "The P-box permutation" (see page 275 and Table 12.7 of Schneier).

The Applicant has also studied the procedures of working-out round subkeys K_1, K_2, ..., K_{16}. According to Schneier, round keys K_1, K_2, ..., K_{16} are generated by means of converting a secret key, on which an operation of fixed transmuting key bits is performed, which depends on the round number but **does not depend on input data**. For a given round, this operation of transmuting key bits is the same for all different datablocks being converted. Following the above fixed key bit transmutation, a fixed compressing key bits transmutation is performed, a result of which is this value of the current round subkey. Fixed compressing key bits transmutation **does not depend on the data begin converted** and remain always the same. Thus, the procedures of forming round keys of DES algorithm also lacks the feature of "prior to carrying out said two-place operation on i-th subblock and subkey, a substitution operation is performed on the subkey **depending on** j-th subblock, where $i \neq j$."
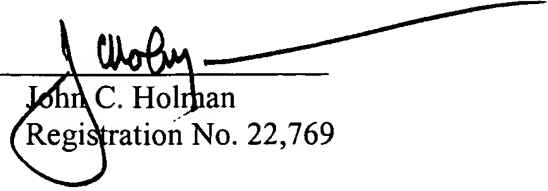
Therefore, the newly presented claim is not anticipated by Schneier and the rejection under 35 U.S.C. § 102 (b) has been overcome. Accordingly, withdrawal of the rejection under 35 U.S.C. § 102 (b) is respectfully requested.

Having overcome all outstanding grounds of rejection, the application is now in condition for allowance, and prompt action toward that end is respectfully solicited.

Respectfully submitted,

JACOBSON HOLMAN PLLC

Date: December 30, 2005   By_____
(202) 638-6666   John C. Holman
400 Seventh Street, N.W.   Registration No. 22,769
Washington, D.C. 20004
Atty. Dkt. No.: P65855US0